

Date: October 15 2008

Publication: Sing Tao Daily, Hong Kong

## Cyber threats are prevalent, Fortinet analyzes new security trends

Enterprises have suffered massive economic losses associated with Internet security and data leakage. More hackers spread viruses and malware in a bid to reap profit.

Derek Manky, security researcher for Fortinet, said with the prevalence of wireless connections, the number of vulnerabilities is on the rise. Manky recommended enterprises to deploy UTM solutions with multiple security functions including firewall, antivirus, antispam, IPSec VPN and web-filtering. Enterprise users are suggested to use a VPN or an SSL site for data transfer and adopt WEP or WPA encryption. Manky also mentioned that cyber crime is growing with financial gain as the main motivation. Enterprises with substantial customer data and credit card transactions are hackers' primary targets. Enterprises are suggested to pursue PCI compliance. Rogue security applications are another emerging area of trickery and scams. Manky reckoned it is imperative to conduct security research and update patches in a timely fashion. Take Fortinet as an example, its seasoned FortiGuard Global Security Research team constantly monitors security vulnerabilities and generates prompt alerts.

### Keep an eye on periodical research reports

Manky recommended a layered security approach to tackle the complex security risks. End-point security should be implemented to help mitigate threats such as smart mobile devices / USB keys / laptops from infecting an internal network. Enterprises should educate employees about the prevalent threats and ensure IT teams remain vigilant at all times.

星島日報 15.10.2008 星期三

企業動態

# 網上陷阱處處

## Fortinet分析保安新趨勢

近年，網絡保安引致企業蒙受鉅大損失，甚至流失大量客戶敏感資料，員工疏忽固引來攻擊，愈來愈多黑客蓄意布局，預謀散播病毒及惡意程式，意圖從中牟利，亦導致網上陷阱處處。

**無縫網絡易暴露個人資料**

Fortinet保安研究工程師 Derek Manky 分析，常見個人侵手法，包括透過下載、SQL injection、網絡釣魚 (phishing)、電郵附件、檔案傳送、網頁瀏覽等過程感染病毒。近年的零時差攻擊 (Zero Day Vulnerabilities) 亦是一大因素，當發現軟件存在漏洞，解決方案公布前，黑客已對弱點發動攻擊。

Manky 表示，無線網絡普及，也新保安漏洞，員工外勤工作，使用無線網絡時，缺乏防火牆保護，黑客趁虛偽造的 WiFi 接入點，一旦發起非法無線網絡用戶，即進行攻擊。部分無線網絡消息皆用無線入資料於手機內，部分又網間不加密，結果暴露客戶資料。

Manky 說，企業可能用防火牆或入侵檢測系統 (UTM)，整合防火牆、防惡功能、惡意軟件、IPSec VPN、動態內容過濾等，以不同網絡安全機制堵截攻擊，也應避免網上公開個人資料，盡量以 VPN 或 SSL 加密傳送資料，以 WEP 或 WPA 加密為 Wi-Fi 存取加密資料。

**網上罪案有上升趨勢**

網上犯罪日發月異，防不勝防，Manky 表示有迹象顯示，網絡罪案有上升趨勢，常見手法是透過大規模電郵寄出惡意郵件及釣魚程式，繼以進入標網站，透過網頁內容，牽動客戶購買員之隱憂而攻擊，也減少所謂 web-home (HTTP) 威脅大為增加，以往犯罪目標只是惡意網頁攻擊，如今則志在牟利，而且針對大量客戶資料的公司為主要目標，誘騙信用卡進行交易的公司，甚為普遍。

Manky 建議企業應遵守業內 PCI 協會所訂下的 PCI-DSS 守則；這是一套全球性的安全標準與架構，要求企業應履行數項安全標準協會 (PCI Security Standards Council) 所訂定下安全規範，目標在保護持卡人敏感資料。

Manky 也建議採取專業與體的監控手法，曾有自稱供職保安程式的駭客，向客戶發出偽造系統受攻擊假訊息，再向客戶催討而下所騙無辜方案，結果讓客戶不意損失了金錢，更建議啟用信用卡資料。

Manky 表示，全面防止網上罪案極為困難，各地法律與守則各異，單是身處外地，執法更加困難。

但以為，保安研究並非由調查者負責重要，所以應定期與被訪者進行緊要合作，及時更新漏洞，以 Fortinet 為例，其成立的 FortiGuard 全球安全研究團隊，定期更新漏洞，不斷尋找保安漏洞，迅速向外發布。

**留意保安組織定期檢查**

定期檢查保安設備，Manky 建議企業可採用分層的保安方案，外圍的防火牆可安裝防病毒、防惡、防垃圾郵件、IPSec VPN、動態內容過濾，客戶所發亦應確保客無法透過可視的 USB 設備、手提電腦、智慧手機或攻擊內部系統。人員疏忽也常導致保安出現疏漏，故員工也應常見威脅，IT 管理隊伍亦應定期更新，確保系統持續。